



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957 Fax: 919.217.5769
<http://www.mercurionsystems.com>

USING EAP AND 802.1X WITH WINDOWS XP FOR WIRELESS LAN SECURITY

Products: Windows XP Professional; Windows 2000 Server or Advanced Server; IEEE 802.1x-compatible wireless network equipment

Overview

Windows XP provides built-in support for 802.1x authentication, a means whereby network access is authenticated on a per-port level before traffic is passed. This allows for a higher level of security, since full network access is predicated upon successful authentication of the computer and/or user. While 802.1x is supported for both wired and wireless network connections, the use of 802.1x in wireless LANs is particularly appealing because it adds a much-needed layer of access control to the wireless LAN. Unauthorized users and/or computers will not be able to simply attach to the wireless LAN and start transmitting. In addition, the use of 802.1x enables the use of dynamic WEP keys, overcoming one of WEP's key weaknesses (static keys).

This technical document discusses how to use 802.1x and EAP-TLS support in Windows XP, IEEE 802.1x-compatible wireless equipment, and Windows 2000's support of EAP through RADIUS (as implemented in the Internet Authentication Service) to provide additional security to a wireless LAN implementation.

More Information

Figure 1, below, shows a network diagram of the components involved in this solution.

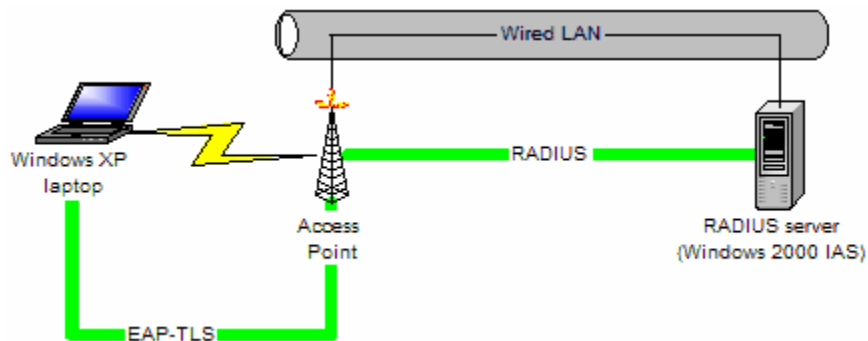


Figure 1. 802.1x components, including EAP-TLS and RADIUS

As noted earlier, the wireless client must be running Windows XP (or another operating system that provides built-in support for 802.1x) or have a vendor-proprietary EAP-based solution (such as Cisco LEAP); however, proprietary EAP-based solutions (such as Cisco LEAP) would not

necessarily be supported by Windows 2000 IAS for authentication. This technical document was written from the perspective of using Windows XP's built-in 802.1x and EAP-TLS support.

There are four major steps involved in setting up 802.1x and EAP-TLS. These steps are:

1. Install and configure IAS (Internet Authentication Service) to provide RADIUS authentication for the 802.1x clients (or supplicants, in 802.1x terminology).
2. Configure the 802.11b wireless access point to support 802.1x, EAP-TLS, and the already-configured RADIUS server.
3. Install certificates for EAP-TLS authentication on the RADIUS server and on the 802.1x clients.
4. Configure the clients to use 802.1x and EAP-TLS authentication.

More information on these four major steps is found in the following sections.

Installing and Configuring IAS

Internet Authentication Service (IAS) is a RADIUS-compatible authentication server for Windows 2000 Server. It can be easily installed through Add/Remove Programs in Control Panel. Once IAS has been installed, use the following steps to configure IAS.

1. Create a new IAS client. This is illustrated on the following page in Figure 2. This screenshot shows the properties for an IAS client. The DNS name of the access point was used instead of the IP address (and DNS resolution was tested), and a shared secret was specified.

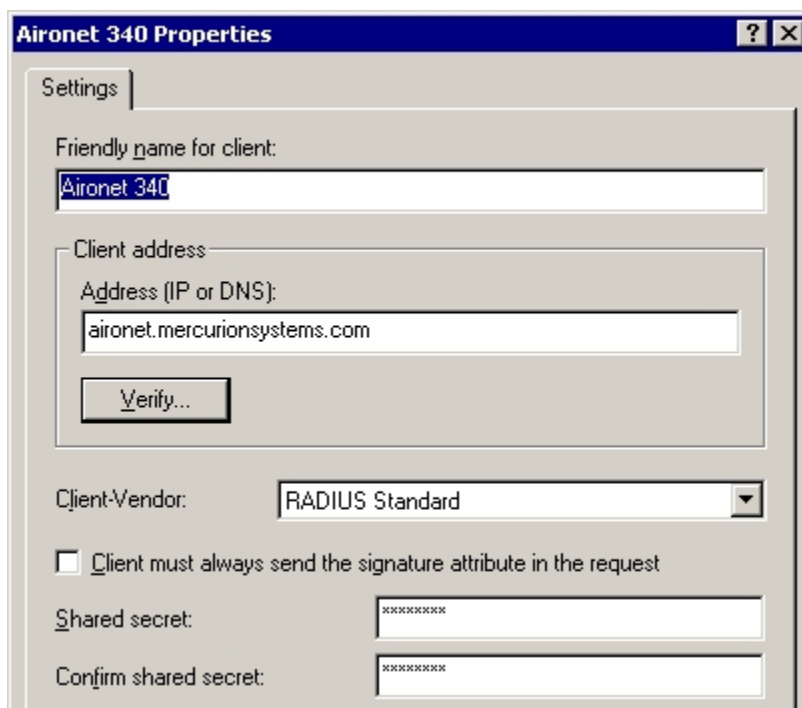


Figure 2. Adding the wireless access point as an IAS client

2. Configure the remote access policy to support EAP-TLS as an authentication type. To do this, modify the existing remote access policy or create a new remote access policy to wireless clients and EAP-TLS. In this technical note, a new remote access policy was created and configured specifically for wireless clients. This new policy is illustrated below in Figure 3, which allows any computer that is a member of the Domain Computers group (which, by default, all Windows XP-based domain members would be) or any user that is a member of the Domain Users group (which, by default, all domain accounts would be) to connect *assuming the correct remote access profile*.

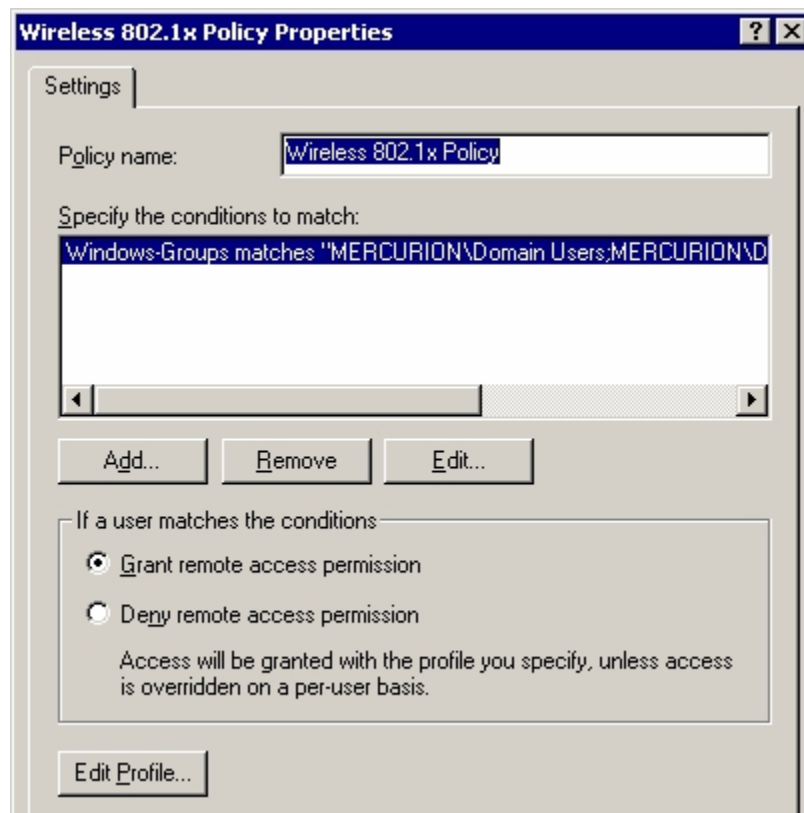


Figure 3. A remote access policy for 802.1x wireless clients

3. Edit the remote access profile (via the “Edit Profile...” button shown in Figure 3) to support 802.11-based wireless clients using EAP. There are two primary steps to this: restricting dial-in media type to wireless, and enabling EAP as an authentication method. These steps are illustrated in Figure 4 and Figure 5, respectively.

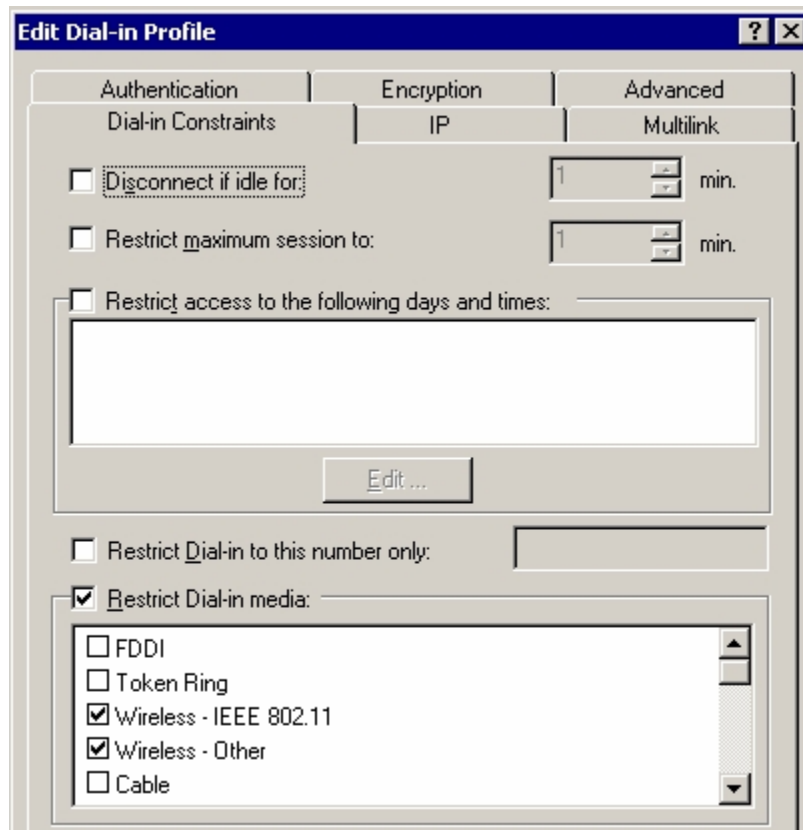


Figure 4. Restricting the dial-in media to wireless

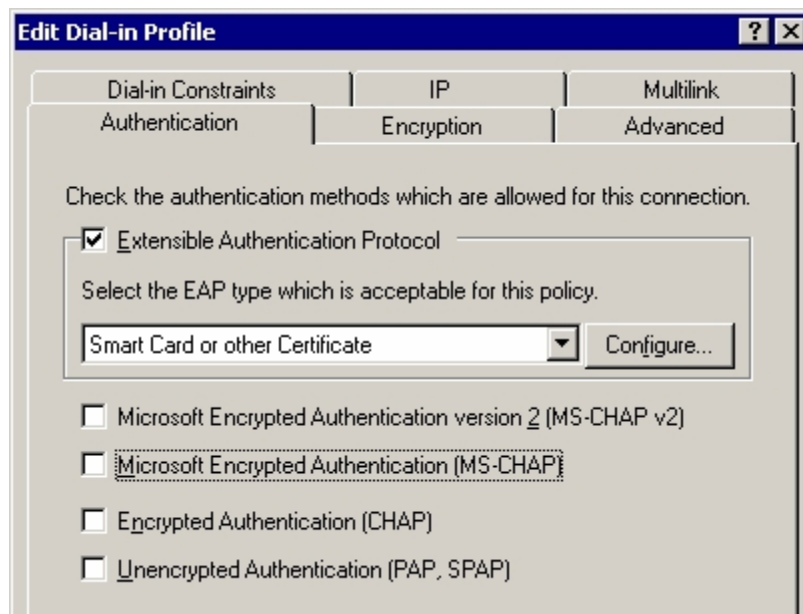


Figure 5. Enabling EAP as an authentication type

Once IAS has been configured, the wireless access point needs to be setup to use EAP and 802.1x for wireless clients.

Configuring the Access Point

Of course, the wireless access point must support 802.1x and EAP in order for this solution to work. The process for configuring the access point will vary from vendor to vendor; these instructions are designed around a Cisco Systems Aironet 340 wireless access point running version 11.21 of the Aironet firmware. (Cisco recommends at least version 11.10T or later of the Aironet firmware.) Consult the vendor's documentation for other manufacturer's access points.

From the access point's main HTML management interface, select Setup > Security > Authentication Server. Figure 6, below, shows the interface for adding an authentication server.

aironet Authenticator Configuration
Cisco AP340 11.21

Map Help

2003/02/24 20:15:54

802.1X Protocol Version (for EAP Authentication): Draft 10

Server Name/IP	Server Type	Port	Shared Secret	Timeout (sec.)
	RADIUS	1812	●●●●●●●●	20
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication				
	RADIUS	1812	●●●●●●●●	20
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication				
	RADIUS	1812	●●●●●●●●	20
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication				
	RADIUS	1812	●●●●●●●●	20
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication				

Apply OK Cancel Restore Defaults

Figure 6. Configuring an authentication server in the access point

All that needs to be added on this screen is the fully-qualified domain name or IP address of the RADIUS server and the shared secret. Keep in mind that the shared secret, which is used for mutual authentication between RADIUS server and RADIUS client, must match on both the wireless access point and the RADIUS server.

Once this information has been entered, clicking on OK takes the user back to the Security screen. From there, click on Radio Data Encryption (WEP) to configure the access point for EAP authentication. This is shown in Figure 7 on the following page.

aironet AP Radio Data Encryption

Cisco AP340 11.21

Map Help

CISCO SYSTEMS

2003/04/14 13:38:48

Use of Data Encryption by Stations is: Full Encryption

Accept Authentication Type: Open Shared Network-EAP

Require EAP:

Transmit With Key	Encryption Key	Key Size
WEP Key 1: <input checked="" type="radio"/>	<input type="text"/>	128 bit
WEP Key 2: <input type="radio"/>	<input type="text"/>	not set
WEP Key 3: <input type="radio"/>	<input type="text"/>	not set
WEP Key 4: <input type="radio"/>	<input type="text"/>	not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

Figure 7. Enabling EAP in the access point

Now that the RADIUS server (the authenticator in 802.1x terminology) and the access point have been configured, the necessary certificates for EAP-TLS authentication need to be installed.

Installing Certificates

EAP-TLS uses certificates for authentication, so certificates must be installed on both the Windows XP clients and the Windows 2000 RADIUS server. Windows 2000's built-in Certificate Services can serve as the certificate authority (CA), or commercial certificates can be purchased from organizations such as VeriSign, Thawte, or Entrust. Because X.509 v3 certificates can be used in so many different ways—IPSec, S/MIME, and EAP-TLS with 802.1x, among others—the creation of an internal public key infrastructure (PKI) may be beneficial in numerous ways. This technical document assumes that an internal CA has been established using Windows 2000's Certificate Services and will be used to issue the certificates.

Two types of certificates will need to be issued:

- A computer certificate, for client authentication of the computer itself
- A user certificate, for client authentication of the user account

The Windows 2000-based IAS server will need only a computer certificate. Each Windows XP-based client will need a computer certificate, and each user account will need a user certificate.

(Note that the Certificates MMC snap-in can be used to issue a request to an Active Directory-integrated CA for the required certificates.)

Configuring the Windows XP Clients

Finally, it is necessary to configure the Windows XP-based clients to use 802.1x when connecting to a wireless network. 802.1x and EAP-TLS support was enhanced in Service Pack 1 for Windows XP; this technical document assumes that Service Pack 1 has been installed. The basic steps are the same for pre-SP1 computers, although the screens will look slightly different.

To enable IEEE 802.1x authentication, check the box marked “Enable IEEE 802.1x authentication for this network” when presented with the list of available wireless networks. In most cases, this is all that is required, and this is illustrated below in Figure 8.

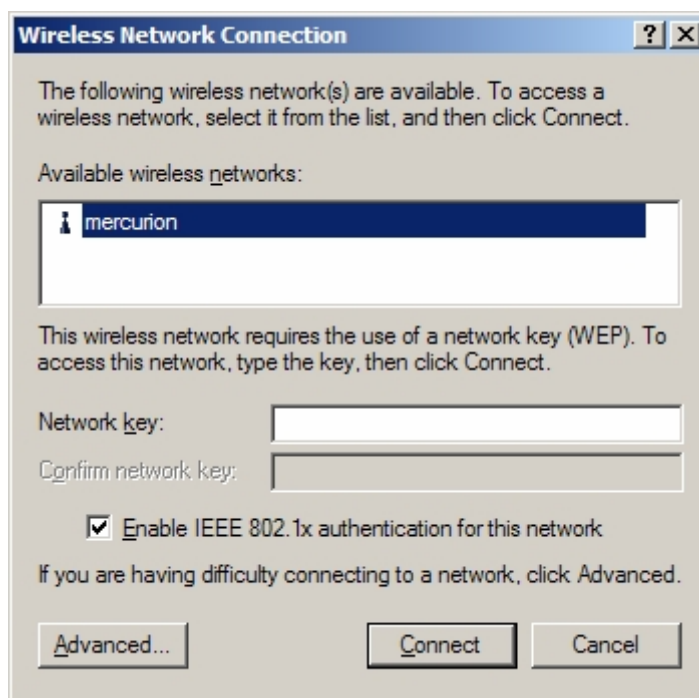


Figure 8. Enabling 802.1x authentication

The “Advanced...” button allows for more in-depth configuration of the 802.1x authentication parameters, but in most cases the default settings will suffice for connecting to a wireless network configured as described in this technical document.

Other Notes

None

Related Articles/Resources

The following Microsoft Knowledge Base articles provide additional information about the use of 802.1x, EAP-TLS, and IAS in this type of situation.

318710: HOW TO: Support Wireless Connections in Windows 2000

306260: Cannot Modify Dial-In Permissions for Computers That Use Wireless Networking

In addition, information regarding the minimum firmware revisions for the Cisco Aironet 340 wireless access point and the correct configuration of the Aironet access point for EAP-TLS authentication was obtained from Cisco's web site at <http://www.cisco.com>.

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.